Representations of finite groups on Riemann-Roch spaces[*]

David Joyner and Will Traves

1-14-2003

Abstract

We study the action of a finite group on the Riemann-Roch space of certain divisors on a curve. If G is a finite subgroup of the automorphism group of a projective curve X and D is a divisor on X stable by G then we show the natural representation of G on Riemann-Roch space $L(D) = L_X(D)$ is a direct sum of irreducible representations of dimension $\leq d$, where d is the size of the smallest G-orbit acting on X. We give an example to show that this is sharp (i.e., that dimension d subrepresentations do occur). We also show, under certain conditions, that $d \geq d_G$, where d_G denotes the largest degree of all irreducible representations of G.

Contents

[*] Research from the first author suported by an NSA-MSP grant. This paper is a longer version of that submitted for publication.

Let X be a smooth projective (irreducible) curve over an algebraically closed field F and let G be a finite subgroup of automorphisms of X over F. We often identify X with its set of F-rational points $X(F)$. If D is a divisor of X which G leaves stable then G acts on the Riemann-Roch space $L(D)$. We ask the question: which (modular) representations arise in this way?

Although this question is interesting in its own right, our motivation for our study lies in coding theory. The construction of Goppa codes uses the Riemann-Roch space $L(D)$ associated to a divisor of a curve defined over a finite field [G]. If G is a cyclic group acting transitively on a basis of $L(D)$ (admittedly an optimistic expectation, but one which gets the idea across) then one might expect that a fast encoding algorithm exists for the associated Goppa codes. Of course, for such an application, one wants F to be finite (and not algebraically closed).

Similar questions have been investigated previously. For example, the action of G on the space of regular differentials, $\Omega^1(X)$ (which is isomorphic to $L(K)$, where K is a canonical divisor [1]). This appears to be first looked at from the representation-theoretic point-of-view by Hurwitz (in the case G is cyclic) and Weil-Chevalley (in general). They were studying monodromy representations on compact Riemann surfaces (for more details and further references, see the book by Breuer [B] and the paper [MP]). Other related works, include those by Nakajima [N], Kani [Ka], and Köck [K], and Borne [Bo1], [Bo2].

[1] The proof of Cor. 2.3 in Köck shows one may construct K in such a way that it is fixed by G and the isomorphism $\Omega^1(X) \cong L(K)$ is G-equivariant.

1 The action of G on $L(D)$

Let X be a smooth projective curve over an algebraically closed field F. Let $F(X)$ denote the function field of X (the field of rational functions on X) and, if D is any divisor on X then the Riemann-Roch space $L(D)$ is a finite dimensional F-vector space given by

$$L(D) = L_X(D) = \{f \in F(X)^\times \mid div(f) + D \geq 0\} \cup \{0\},$$

where $div(f)$ denotes the (principal) divisor of the function $f \in F(X)$. Let $\ell(D)$ denote its dimension. We recall the Riemann-Roch theorem,

$$\ell(D) - \ell(K - D) = \deg(D) + 1 - g,$$

where K denotes a canonical divisor and g the genus [2].

The action of $\mathrm{Aut}(X)$ on $F(X)$ is defined by

$$\begin{array}{rccc} \rho: & \mathrm{Aut}(X) & \longrightarrow & \mathrm{Aut}(F(X)), \\ & g & \longmapsto & (f \longmapsto f^g) \end{array}$$

where $f^g(x) = (\rho(g)(f))(x) = f(g^{-1}(x))$.

Note that $Y = X/G$ is also smooth and $F(X)^G = F(Y)$.

Of course, $\mathrm{Aut}(X)$ also acts on the group $Div(X)$ of divisors of X, denoted $g(\sum_P d_P P) = \sum_P d_P g(P)$, for $g \in \mathrm{Aut}(X)$, P a prime divisor, and $d_P \in \mathbb{Z}$. It is easy to show that $div(f^g) = g(div(f))$. Because of this, if $div(f) + D \geq 0$ then $div(f^g) + g(D) \geq 0$, for all $g \in \mathrm{Aut}(X)$.

If the action of $G \subset \mathrm{Aut}(X)$ on X leaves $D \in Div(X)$ stable then we denote the associated representation of G in $L(D)$ by ρ:

$$\rho : G \to \mathrm{Aut}(L(D)).$$

2 Examples and special cases

Before tackling the general case, we study the Riemann-Roch representations of G when $X = \mathbb{P}^1$ or D is the canonical divisor.

[2] We often also use g to denote an element of an automorphism group G. Hopefully, the context will make our meaning clear.

2.1 The canonical embedding

Let K denote a canonical divisor of X, so $\deg(K) = 2g-2$ and $\dim(L(K)) = g$. Let $\{\kappa_1, ..., \kappa_g\}$ denote a basis for $L(K)$. If the genus g of X is at least 2 then the morphism

$$\begin{array}{rcl} \phi : X & \longrightarrow & \mathbb{P}(\Omega^1(X)) \cong \mathbb{P}^{g-1} \\ x & \longmapsto & (\kappa_1(x) : ... : \kappa_g(x)) \end{array}$$

defines an embedding, the "canonical embedding", and ϕ is called the "canonical map". It is known that $L(K)$ is isomorphic (as F-vector spaces) to the space $\Omega^1(X)$ of regular Weil differentials on X. This is contained in the space of all Weil differentials, $\Omega(X)$. (In the notation of [Sti], $\Omega^1(X) = \Omega(X)(0)$.) Since G acts on the set of places of F, it acts on the adele ring of F, hence on the space $\Omega(X)$.

Now, even though K might not be fixed by G, there is an action of G on $L(K)$ obtained by pulling back the action of G on $\Omega^1(X)$ via an isomorphism $L(K) \cong \Omega^1(X)$.

The group $\mathrm{Aut}(X)$ acts on X and on its image $Y = \phi(X)$ under an embedding $\phi : X \to \mathbb{P}^n$. If ϕ arises from a very ample linear system then an automorphism of Y may be represented (via the linear system) by an element of $PGL(n+1, F)$ acting on $\mathbb{P}^n$ which preserves Y (see §8.6 of [SKKT] for more details on such embeddings). For instance, if D is any divisor with $\deg(D) > 2g$ then the morphism

$$\begin{array}{rcl} \phi : X & \to & \mathbb{P}^{n-1} \\ x & \longmapsto & (f_1(x) : ... : f_n(x)) \end{array}$$

defines an embedding, where $\{f_1, ..., f_n\}$ is a basis for $L(D)$ (see, for example, Stepanov [St], §4.4, or [SKKT]). This projective representation of G on $L(D)$ exists independent of whether or not D is left stable by G.

Example 1 *Let $X = \mathbb{P}^1/\mathbb{C}$ have projective coordinates $[x : y]$, let $G = \{1, g\}$, where $g(x/y) = y/x$, and let $D = 2[1 : 0] - [0 : 1]$, so $L(D)$ has basis $\{x/y, x^2/y^2\}$. Then $g(x/y) = (y/x)^3(x^2/y^2)$ and $g(x^2/y^2) = (y/x)^3(x/y)$. Thus, as an element of $PGL(2, \mathbb{C})$, g is $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.*

Suppose, for example, X is non-hyperelliptic of genus ≥ 3 and ϕ arises from the canonical embedding. In this case, we have (a) the projective representation

$$\pi : G \to \mathrm{Aut}(\mathbb{P}(\Omega^1(X)))$$

(acting on the canonical embeding of X) and (b) the projective representation obtained by composing the "natural" representation $G \to \mathrm{Aut}(\Omega^1(X))$ with the quotient map $\mathrm{Aut}(\Omega^1(X)) \to \mathrm{Aut}(\Omega^1(X)/F^\times) = \mathrm{Aut}(\mathbb{P}(\Omega^1(X)))$. These two representations are the same.

Remark 1 *For further details on the representation $G \to \mathrm{Aut}(\Omega^1(X))$, see for example, the Corollary to Theorem 2 in [K], Theorem 2.3 in [MP], see pages 750-751 in Lewittes [Le]. or the book by T. Breuer [B].*

2.2 The projective line

Let $X = \mathbb{P}^1/F$, so $\mathrm{Aut}(X) = PGL(2, F)$, where F is algebraically closed. Let $\infty \in X$ denote the element corresponding to the localization $F[x]_{(1/x)}$. In this case, the canonical divisor is given by $K = -2\infty$, so the Riemann-Roch theorem becomes

$$\ell(D) - \ell(-2\infty - D) = \deg(D) + 1.$$

It is known (and easy to show) that if $\deg(D) < 0$ then $\ell(D) = 0$ and if $\deg(D) \geq 0$ then $\ell(D) = \deg(D) + 1$.

Example 2 *Most of the examples below were computed using MAGMA 2.8 [MAGMA].*

Let $F = \overline{\mathbb{F}_5}$. Let $P_1 = [1:0]$, $P_2 = [1:1]$, $P_3 = [1:2]$, $P_4 = [1:3]$, $P_5 = [1:4]$, $\infty = [0:1]$.

D	*basis for* $L(D)$
$2\infty - 2P_3$	$(x+3)^2$
$\infty - 2P_3$	$\emptyset$
$2\infty - 2P_1$	x^2
$3\infty - 2P_1$	x^2, x^3
$3\infty - 2P_5$	$x(x+1)^2, (x+1)^2$
$6P_1 - 3P_3 - 2P_5$	$x^{-5}(x+3)^3(x+1)^2$, $x^{-6}(x+3)^3(x+1)^2$
$7P_1 - 3P_3 - 2P_5$	$x^{-5}(x+3)^3(x+1)^2$, $x^{-6}(x+3)^3(x+1)^2,\ x^{-7}(x+3)^3(x+1)^2$
$-2\infty + P_1 - 3P_3 + 2P_5$	$\emptyset$
$-2\infty + 3P_1 - 3P_3 + 3P_5$	$x^{-2}(x+1)^{-3}(x+3)^3,\ (x+1)^{-3}x^{-3}(x+3)^3$
$-2\infty + 3P_2 - 3P_3 + 3P_5$	$x(x+1)^{-3}(x+4)^{-3}(x+3)^3$, $(x+1)^{-3}(x+4)^{-3}(x+3)^3$
$P_1 + 3P_3 - 2P_5$	$x(x+3)^{-3}(x+1)^2,\ (x+3)^{-3}(x+1)^2$, $x^{-1}(x+3)^{-3}(x+1)^2$
$-P_1 + 3P_2 - 2P_3$	$x(x+3)^{-3}(x+1)^2$
$7\infty - 2P_3 - 2P_5$	$x^3(x+3)^2(x+1)^2,\ x^2(x+3)^2(x+1)^2$, $x(x+3)^2(x+1)^2,\ (x+3)^2(x+1)^2$
$3\infty + 3P_2 - 2P_3 - 2P_5$	$p(x) = x^2(x+4)^{-3}(x+3)^2(x+1)^2$, $xp(x),\ x^2p(x)$

In the case of the projective line, there is another way to see the action ρ of $\mathrm{Aut}(X)$ on $F(X)$. Each function $f \in F(X)$ may be written uniquely as a rational function $f(x) = p(x)/q(x)$, where $p(x)$ and $q(x)$ are polynomials that factor as the product of linear polynomials. Assume that both p and q are monic, and assume that the linear factors of them are as well. The group $\mathrm{Aut}(X)$ "acts" on the set of such functions f by permuting its zeros and poles according to the action of G on X. (We leave aside how G acts on the constants, so this "action" is not linear.) We call this the "permutation action", $\pi : g \longmapsto \pi(g)(f) = f_g$, where $f_g(x)$ denotes the function f with zeros and poles permuted by g.

Lemma 3 *If $G \subset \mathrm{Aut}(X)$ leaves $D \in Div(X)$ stable then*

$$\pi(g)(f) = c\rho(g)(f),$$

for some constant c.

proof: Note that, by definition, $div(\pi(g)(f)) = div(f_g) = g(div(f))$, for $g \in G$ and $f \in L(D)$. Since $div(\pi(g)(f)) = g(div(f)) = div(\rho(g)(f)) = div(f^g)$, the functions f^g and f_g must differ by a constant factor. □

The above lemma is useful since it is easier to deal with π than ρ in this case.

A basis for the Riemann-Roch space is explicitly known for $\mathbb{P}^1$. For notational simplicity, let

$$m_P(x) = \begin{cases} x, & P = [1:0] = \infty, \\ (x-p)^{-1}, & P = [p:1]. \end{cases}$$

Lemma 4 *Let $P_0 = \infty = [1:0] \in X$ denote the point corresponding to the localization $F[x]_{(1/x)}$. For $1 \leq i \leq s$, let $P_i = [p_i : 1]$ denote the point corresponding to the localization $F[x]_{(x-p_i)}$, for $p_i \in F$. Let $D = \sum_{i=0}^{s} a_i P_i$ be a divisor, $a_k \in \mathbb{Z}$ for $0 \leq k \leq s$.*

(a) If D is effective then

$$\{1, m_{P_i}(x)^k \mid 1 \leq k \leq a_i, 0 \leq i \leq s\}$$

is a basis for $L(D)$.

(b) If D is not effective but $deg(D) \geq 0$ then write $D = dP + D'$, where $deg(D') = 0$, $d > 0$, and P is any point. Let $q(x) \in L(D')$ (which is a 1-dimensional vector space) be any non-zero element. Then

$$\{m_P(x)^i q(x) \mid 0 \leq i \leq d\}$$

is a basis for $L(D)$.

(c) If $deg(D) < 0$ then $L(D) = \{0\}$.

The first part is Lemma 2.4 in [L]. The other parts follow from the definitions and the Riemann-Roch theorem.

Remark 2 *The obvious analog of the second part of the above lemma is false in the case of a curve of genus $g > 1$. In this case, if $D \neq 0$ is a divisor of degree 0 then $L(D) = \{0\}$. (This is a consequence of Corollary 4.9 (iv) in [St], for example.)*

Example 5 *If $F = \mathbb{C}$ and we identify X with the "Riemann sphere" $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ then we may regard the automorphisms as linear fractional transformations.*

Let G be the group generated by the map $\phi(x) = 1/x$, $x \in \hat{\mathbb{C}}$. Let P_1 be represented by $x_1 = 1 + i$, let P_2 be represented by $x_2 = \frac{1}{2} - \frac{i}{2}$, and let P_3 be represented by $x_3 = 1$.

1. *Let $D = P_1 + P_2$. Then G stabilizes D and $L(D)$ has basis $\{e_1 = 1, e_2 = 1/(x - x_1), e_3 = 1/(x - x_2)\}$. The map ϕ fixes e_1, sends e_2 to $-x_2e_1 - x_2^2e_3$ and e_3 to $-x_1e_1 - x_1^2e_2$. With respect to this basis, the representation of G on $L(D)$,*
$$\rho : G \to \mathrm{Aut}(L(D))$$
is determined by
$$\rho(\phi) = \begin{pmatrix} 1 & -x_2 & -x_1 \\ 0 & 0 & -x_1^2 \\ 0 & -x_2^2 & 0 \end{pmatrix}.$$

2. *Let $D = P_1 + P_2 - P_3$. Then G stabilizes D and $L(D)$ has basis $\{e_1 = (x - 1)/(x - x_1), e_2 = (x - 1)/(x - x_2)\}$. With respect to this basis, the representation ρ of G on $L(D)$ is determined by*
$$\rho(\phi) = \begin{pmatrix} 0 & x_2 \\ x_1 & 0 \end{pmatrix}.$$
This looks like it might be a non-diagonal representation. However, with respect to the basis $\{e_1 = \frac{(x-1)^2}{(x-x_1)(x-x_2)}, e_2 = \frac{x-1}{(x-x_1)(x-x_2)}\}$, the representation ρ is diagonal.

In general, we have the following result.

Theorem 6 *Let X, $G \subset \mathrm{Aut}(X) = PGL(2, F)$, and $D = \sum_{i=0}^{s} a_iP_i$ be a divisor as above. Assume F is algebraically closed and that the order of G is relatively prime to the characteristic of F. Let $\rho : G \to \mathrm{Aut}(L(D))$ denote the associated representation. This acts trivially on the constants (if any) in $L(D)$; we denote this action by 1. Let $S = \mathrm{supp}(D)$ and let*
$$S = S_1 \cup S_2 \cup ... \cup S_m$$
be the decomposition of S into primitive G-sets.

(a) If D is effective then

$$\rho \cong 1 \oplus_{i=1}^m \rho_i,$$

where ρ_i is a monomial representation on the subspace

$$V_i = \langle m_P(x)^{\ell_j} \mid 1 \leq \ell_j \leq a_j,\ P \in S_i \rangle,$$

satisfying $dim(V_i) = \sum_{P_j \in S_i} a_j$, for $1 \leq i \leq m$. Here $\langle ... \rangle$ denotes the vector space span.

(b) If $deg(D) > 0$ but D is not effective then ρ is the direct sum of 1-dimensional subrepresentations.

In particular, the representation of G on $L(D)$ is semi-simple.

proof: We prove the first part first.

Fix for now an i satisfying $1 \leq i \leq m$. Consider the subspace L_i of $L(D)$ spanned by the functions $f_P(z) = 1/(z - z_P)^{e(P,D)}$, where $P \in S_i$, $e(P,D) \geq 0$, and $z_P \in F$ represents $P \in X$ (unless $P = \infty$, in which case replace z_P by 0 and $e(P,D)$ by $-e(P,D)$). Since G acts by permuting the points in S_i transitively, this action induces an action ρ_i on L_i. This action on L_i is a permutation representation since it is one on S_i. It is irreducible since the action on S_i is transitive, by definition. Clearly $\oplus_{i=1}^m \rho_m$ is a subrepresentation of ρ. For dimension reasons, it must be all of ρ, modulo the constants.

This proves the first part.

It remains to prove the second part.

Let $P \in \text{supp}(D)$ and let

$$G_P = \{g \in G \mid g(P) = P\}$$

denote the stabilizer of P in G (i.e., the decomposition group of the Galois covering $X \to Y = X/G$ at P). In the construction of a basis in Lemma 4, take the P in Lemma 4 to be as above. By this construction and Lemma 3, the action of G_P on S induces a "diagonal action" on a basis of $L(D)$.

Since D is not effective, we may write $D = D^+ - D^-$, where D^+ and D^- are non-zero effective divisors. The action of G must preserve D^+ and D^-. There is a corresponding partitioning $S = S^+ \cup S^-$, where $S^+ = \text{supp}(D^+)$ and $S^- = \text{supp}(D^-)$. Embed G into the symmetric group of S, $G \hookrightarrow Symm(S)$. Since the action of G must preserve S^+ and S^-, this embedding factors through $Symm(S^+) \times Symm(S^-)$. Write this factorization as

$G \subset G^+ \times G^-$. Note G as a subdirect product of $G^+ \times G^-$ and that the action of G on $L(D)$ extends to an action of $H = G^+ \times G^-$. (G is not always a subdirect product of $Symm(S^+) \times Symm(S^-)$.) Call this extension of ρ to H, ρ_H. If $P \in S^+$ then $G^- \subset G_P$ (identifying G^- with a subgroup of G), since all the elements of G^- fix such a P, so $(G_P)^- \cong G^-$. Similarly, if $P \in S^-$ then $(G_P)^+ \cong G^+$ since all the elements of G^+ fix such a P.

Combining these two paragraphs, we see that $L(D)$ has a basis on which G^+ acts "diagonally". Similarly for G^-.

Let π denote an irreducible subrepresentation of ρ_H. Our hypotheses imply that π is of the form $\pi^+ \otimes \pi^-$, where π^+ is an irreducible representation of G^+ and π^- is an irreducible representation of G^-. By the above discussion, $\dim(\pi^+) = \dim(\pi^-) = 1$, so $\dim(\pi) = \dim(\pi^+) \cdot \dim(\pi^-) = 1$. Sinve every irreducible subrepresentation of ρ_H is 1-dimensional, the same must be true for ρ.

This completes the proof of the second part. □

3 The general case

The goal of this section is to prove an analog of Theorem 6 for any smooth projective curve X over an algebraically closed field F.

Example 7 *Most of the examples below were computed using MAGMA 2.8 [MAGMA].*

Let X be the plane curve defined by the affine equation $y^2 = x(x-1)(x-2)$ over $F = \overline{\mathbb{F}_5}$. This is an elliptic curve. Let $P_1 = (0:1:0) = \infty$, $P_2 = (0:0:1)$, $P_3 = (2:0:1)$, $P_4 = (4:3:1)$, $P_5 = (4:2:1)$, $P_6 = (3:4:1)$, $P_7 = (3:1:1)$, $P_8 = (1:0:1)$.

D	*basis for* $L(D)$
∞	1
2∞	$1, x$
3∞	$1, x, y$
4∞	$1, x, y, x^2$
$P_1 + P_2 + ... + P_8$	$x^3y/(x^4+4)$, $x^2y/(x^4+4)$, $xy/(x^4+4)$, $y/(x^4+4)$, $y/(x^5+4x)$, 1, $(x+3)/(x^2+3x+2)$, $1/(x^2+3x+2)$
$P_2 + ... + P_8$	$x^2y/(x^4+4)$, $xy/(x^4+4)$, $y/(x^4+4)$, $y/(x^5+4x)$, 1, $(x+3)/(x^2+3x+2)$, $1/(x^2+3x+2)$
$-P_1 + P_2 + ... + P_8$	$x^2y/(x^4+4)$, $xy/(x^4+4)$, $y/(x^4+4)$, $y/(x^5+4x)$, $(x+3)/(x^2+3x+2)$, $1/(x^2+3x+2)$
$-2P_1 + P_2 + ... + P_8$	$xy/(x^4+4)$, $y/(x^4+4)$, $y/(x^5+4x)$, $(x+3)/(x^2+3x+2)$, $1/(x^2+3x+2)$
$-3P_1 + P_2 + ... + P_8$	$xy/(x^4+4)$, $y/(x^4+4)$, $y/(x^5+4x)$, $1/(x^2+3x+2)$
$-4P_1 + P_2 + ... + P_8$	$y/(x^4+4)$, $y/(x^5+4x)$, $1/(x^2+3x+2)$
$-5P_1 + P_2 + ... + P_8$	$y/(x^4+4)$, $y/(x^5+4x)$
$-6P_1 + P_2 + ... + P_8$	$y/(x^5+4x)$
$-7P_1 + P_2 + ... + P_8$	$y/(x^5+4x)$
$-8P_1 + P_2 + ... + P_8$	0

Incidently, since $D = -7P_1 + P_2 + ... + P_8$ is degree 0 but $L(D)$ is non-zero, it must be the canonical divisor (up to linear equivalence) by [Sti], Proposition I.6.2.

Next, we at least partially answer the question: How much of the information about the case of $\mathbb{P}^1$ can be "pulled-pack" to a cover $X \to \mathbb{P}^1$?

3.1 Pull-backs of a Riemann-Roch space

Let X be a smooth curve over F and $\phi : X \to \mathbb{P}^1$ be a non-constant morphism of degree $d = \deg(\phi)$.

Example 8 *(Lorenzini [L], §IX.8; Stichtenoth [Sti], §§VI.2-Vi.33) Assume F is algebraically closed and $char(F) \neq 2$. Pick distinct $a_1, a_2, ..., a_s \in F$, pick any positive integers $r_1, ..., r_s$, choose $c \in F^\times$, and let*

$$f(x,y) = y^d - c\prod_{i=1}^{s}(x-a_i)^{r_i}.$$

Then the curve X defined by the affine equation $f(x,y) = 0$ is irreducible and the morphism $\phi : X \to \mathbb{P}^1$ induced by the coordinate function x is ramified only over the points $P_i = [a_i : 1] \in \mathbb{P}^1$, $1 \leq i \leq s$. The fiber in X over P_i has $d/gcd(d, r_i)$ elements and

$$genus(X) = \frac{1}{2}[(s-2)(d-1) - \sum_{i=1}^{s}(gcd(d,r_i)-1)].$$

Example 9 *One way to find an example of a group acting on X which preserves a divisor on X to consider a Galois covering $\phi : X \to \mathbb{P}^1$ with Galois group $G = \mathrm{Aut}(X/\mathbb{P}^1)$. If $D \in Div(\mathbb{P}^1)$ then the action of G on $Div(X)$ stabilizes ϕ^*D. Indeed, roughly speaking, G acts by permuting the fibers of ϕ. It also acts on $L_X(\phi^*D)$ and leaves stable the image of $L(D)$ in $L_X(\phi^*D)$:*

$$L_X(\phi^*D)^G \cong L(D).$$

See [TV], Ex. 2.2.16, page 150 (which is more general than the result we stated above), and §2 of Kani [Ka].

In particular, the multiplicity of the trivial (1-dimensional) representation of G on $L_X(\phi^*D)$ is $\ell(D) = \deg(D) + 1$.

Let $D \in Div(\mathbb{P}^1)$ and consider the Riemann-Roch space $L(D) = L_{\mathbb{P}^1}(D)$ of D. Define its pull-back by

$$\phi^*L(D) = \{f \in F(X)^* \mid f = g \circ \phi, \text{ some } g \in L(D)\}.$$

Note that the map $g \longmapsto g \circ \phi$ defines a vector space isomorphism $L(D) \cong \phi^*L(D)$. Thus, $L(D)$ may be regarded as a subspace of $L_X(\phi^*D)$.

The morphism ϕ induces a map $\phi^* : Div(\mathbb{P}^1) \to Div(X)$, defined on points by

$$\phi^*p = \sum_{\{P \in X \mid \phi(P)=p\}} e_{P/p}P,$$

where $e_{P/p}$ denotes the ramification index, and extended to the divisor group by linearity ([L], page 267). This map preserves the effective divisors. We can consider the Riemann-Roch space of the pull-back of a divisor:

$$L_X(\phi^*D) = \{f \in F(X)^* \mid div(f) + \phi^*D \geq 0\}.$$

A natural question is to ask how the pull-back of the Riemann-Roch space is related to the Riemann-Roch space of the pull-back. The next result answers this. For later reference, we shall formulate the result a little more generally.

Proposition 10 *Let $\phi : X \to Y$ be a morphism of curves. For any divisor D of Y, $\phi^*L_Y(D) \subset L_X(\phi^*D)$.*

proof: If $f \in \phi^*L_Y(D)$ then $f = g \circ \phi$, for some $g \in L_Y(D)$. We know then that $div(g) + D \geq 0$. This implies $\phi^*(div(g)) + \phi^*D \geq 0$ since ϕ^* preserves the effective divisors. But $div(f) = div(g \circ \phi) = \phi^*(div(g))$, so $div(f) + \phi^*D \geq 0$. □

Corollary 11 *Let $\phi : X \to Y$ be a birational morphism of curves. For any divisor D of Y, $\phi^* L_Y(D) \cong L_X(\phi^* D)$. Moreover, if G acts on both X and Y, preserves D, and if ϕ is G-equivariant then G stabilizes $\phi^* D$ and the isomorphism is G-equivariant.*

proof: Let $E = \phi^* D$ and $\psi = \phi^{-1}$. We claim that $\psi^* E = D$. For all points P of X, we have $\psi(\phi(P)) = P$; from the definition of ϕ^* and ψ^*, this identity extends to divisors. This claim and the proposition give $\phi^* L_Y(D) \subset L_X(E)$ and $\psi^* L_X(E) \subset L_Y(\psi^* E) = L_Y(D)$. Therefore,

$$\psi^* \phi^* L_Y(D) \subset \psi^* L_X(E) \subset L_Y(D).$$

Since $\phi^* : F(Y) \to F(X)$ is a field isomorphism and $\psi^* = (\phi^*)^{-1}$, the desired isomorphism follows.

If ϕ satisfies $g\phi(P) = \phi(gP)$, for all points P of X, and if G leaves D stable then it must also do so to $\phi^* D$. This G action on the Riemann-Roch spaces must commute with the pull-backs ϕ^* and ψ^*, by their definitions, so the isomorphism is G-equivariant. □

Recall that all non-singular projective curves X are birationally equivalent to a (possibly singular) plane curve. In some cases, this last result allows us to reduce the problem of explicitly determining the representations of G on $L_X(D)$ to the case where X is a (projective) plane curve embedded in $\mathbb{P}^2$. This is useful for us since the computations are much simpler in the planar case. However, not all cases can be covered in this way, since the above result requires that G act on both X and its plane model, which may not always be possible.

3.2 A computational method

We present a method for determining the "one-point spaces" $L(mP)$ for a plane curve X. Suppose that X has an affine model defined by $f(x, y) = 0$, where $f \in F[x, y]$.

Let $D = \sum_P d_P P$, where $d_P = ord_P(D)$. Fix a point P in the support of D and let π denote a local uniformizer at P.

Suppose P is the point in $X(F)$ at infinity. In the π-adic completion $\hat{\mathcal{O}_P}$ of the local coordinate ring of X at P, $\mathcal{O}_P$, the local coordinates x and y may be written

$$x = u_x \pi^{-M}, \qquad y = u_y \pi^{-N}$$

for some units u_x and u_y in $\hat{\mathcal{O}_P}$, and for some integers $M = M(P) \in \mathbb{Z}$ and $N = N(P) \in \mathbb{Z}$. Then $x^r y^s$ has a pole of order $rM+sN$ at P if $rM+sN > 0$, and a zero of order $|rM+sN|$ at P if $rM+sN < 0$. A monomial $x^r y^s \in F(X)$ (with $R \geq 0$ and $s \geq 0$) belongs to $L(D)$ if and only if

$$rM(P) + sN(P) \leq d_P, \tag{1}$$

for all $P \in \mathrm{supp}(D)$.

3.2.1 Examples

Example 12 *Suppose X is given in affine coordinates by $y^2 = x(x-1)(x-2)$ and $F = \mathbb{F}_5$. Let $P = [0 : 1 : 0]$. Then we have*

$$x = u_x \pi^{-2}, \qquad y = u_y \pi^{-3}$$

for some units u_x and u_y. (Substitute $x = u_x \pi^a$ and $y = u_y \pi^b$ into $y^2 = x(x-1)(x-2)$ and solve for a, b.)

A monomial $x^r y^s$ is in $L(5P)$ if and only if $2r + 3s \leq 5$, $r \geq 0$, $s \geq 0$ (these last two inequalities are to avoid having a pole at $[0 : 0 : 1]$)). These give $(r, s) \in \{(0,0), (1,0), (0,1), (1,1), (2,0)\}$, so

$$1, x, y, x^2, xy \in L(5P).$$

In fact, these functions form a basis of $L(5P)$.

Example 13 *Let C be the curve $y^3 = x + x^2$ over an algebraically closed field F of characteristic $\neq 3$. As a projective curve, C is given by*

$$Y^3 - X^2 Z - X Z^2 = 0.$$

There is a morphism $\phi : C \to \mathbb{P}^1$ given by $[X : Y : Z] \longmapsto (X : Z)$. The map $g : [X : Y : Z] \longmapsto [X : \zeta Y : Z]$, where $1 \neq \zeta \in F$ is a cube root of 1, generates an action of the group $G \cong \mathbb{Z}/3\mathbb{Z}$ on C. (With G acting trivially on $\mathbb{P}^1$, the morphism ϕ is G-equivariant. Note the map swapping X and Z is also an automorphism of C, though it is not in the Galois group of $C \to \mathbb{P}^1$ so we shall not use it.)

The map ϕ is ramified over $p_1 = [0 : 1]$, $p_2 = (1 : 0)$, $p_3 = (-1 : 1)$, with preimages $P_1 = \phi^{-1}(p_1) = (0 : 0 : 1)$, $P_2 = \phi^{-1}(p_2) = (1 : 0 : 0)$,

$P_3 = \phi^{-1}(p_3) = (-1:0:1)$. The action of G fixes P_i, $i = 1,2,3$. Let $p \in \mathbb{P}^1$ be arbitrary and let

$$D = \phi^*(p),$$

so typically D is a sum of three points (the preimages of p) but when $p = p_i$, D is of the form $3P_i$. By Example 9, the trivial representation of G is contained in $L(D)$ with multiplicity 4. Thus, the G-modules $L(P)$ are all trivial.

Example 14 *Let $k = \mathbb{C}$ denote the complex field and let $X(N)$ denote the modular curve associated to the principle congruence group $\Gamma(N)$ (see for example Stepanov, [St], chapter 8). The group $PSL(2, \mathbb{Z}/N\mathbb{Z})$ is contained in the automorphism group of $X(N)$. Over an algebraically closed field of characteristic zero, if $p \geq 7$ is prime then $Aut(X(p)) \cong PSL(2, \mathbb{F}_p)$, where $\mathbb{F}_p$ denotes the Galois field of p elements.*

Example 15 *Suppose X is given in affine coordinates by $y^2 = x^3 + 1$ and $F = \mathbb{F}_5$. Let $P = [0:1:0]$. Homogenize X to $y^2z = x^3 + z^3$ to find that there is only one point at infinity (where $z = 0$), P. In this example, the group*

$$G = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

acts by

$$(a,b,c) \cdot [x:y:z] = [\zeta^a x : \eta^b y : z],$$

for $(a,b,c) \in G$. The coordinate function x on X now becomes the homogeneous function x/z on the projective curve. Considering the chart $\{y \neq 0\}$, we can form an affine isomorphism of the neighborhood of P to the affine curve $z = x^3 + z^3$ (where P is sent to $O = (0,0)$). Now the order of the original x at infinity is just the order of x/z at $(0,0)$ and

$$ord_O(x/z) = ord_O(x) - ord_O(z) = 1 - ord_O(\frac{x^3}{1-z^2}) = 1 - 3 = -2.$$

So x has a pole of order 2 at infinity (as in the above example). Here we used x as the uniformizing parameter: O is a simple (ie. smooth) point on $z = x^3 + z^3$ and so it defines a discrete valuation ring: $F[x,z]_{(x,z)}/(z - x^3 - z^3)$. The maximal ideal $m = (x,z) = (x)$ so x is the uniformizing parameter and we can use it to give an order function.

Similarly, one can compute that the order of y is the order of $1/z$ at O and this is just -3.

Example 16 *For instance, look at $X : y^2 = x^5 + x^3 + 4$, a hyperelliptic curve of genus 2. Again there is only one point at infinity $(0:1:0)$ but now it is a singular point* [3]*. Consider again the chart $\{y \neq 0\}$, and the point $O = (0,0)$ that P is sent to. We can replace the orders by intersection multiplicities (see Fulton [F], pages 74-81, for example):*

$$\begin{aligned} ord_O(x) = I(O, V(x) \cap V(z^3 - x^5 - x^3z^2 - 4z^5) = \\ I(O, V(x) \cap V(z^3 - 4z^5)) = ord_O^{V(x)}(z^3 - 4z^5) = 3, \end{aligned}$$

and

$$\begin{aligned} ord_O(z) = I(O, V(z) \cap V(z^3 - x^5 - x^3z^2 - 4z^5) \\ = I(O, V(z) \cap V(x^5)) = ord_O^{V(z)}(x^5) = 5. \end{aligned}$$

Thus $ord_O(x/z) = 3 - 5 = -2$.

Since y restricts to 1 in the affine chart, $ord_O(y) = ord_O(1) = 0$, so

$$ord_O(y/z) = 0 - 5 = -5$$

On the original curve X, x has a pole of order 2 at infinity and y has a pole of order 5 at infinity.

Remark 3 *Let (x_0, y_0) represent the projective point $P = [x_0 : y_0 : 1] \in X(F)$. We can write*

$$x - x_0 = u_x \pi^M \qquad y - y_0 = u_y \pi^N$$

for some units u_x, u_y and some integers $M = M(P) \in \mathbb{Z}$ and $N = N(P) \in \mathbb{Z}$. A monomial $(x - x_0)^r (y - y_0)^s \in F(X)$ belongs to $L(D)$ if and only if

$$rM(P) + sN(P) + d_P \geq 0,$$

for all $P \in \mathrm{supp}(D)$.

Example 17 *Suppose X is given in affine coordinates by $y^2 = x(x-1)(x-2)$ and $F = \mathbb{F}_5$. Let $P = (2:0:1)$. Then*

$$x = 2 + u_x \pi^2, \qquad y = u_y \pi,$$

[3] This means that we don't have a discrete valuation ring at O as in the above example, so we can't compute the orders using the uniformizing parameter directly.

for some units u_x, u_y. (As above, substitute $x = 2 + u_x\pi^a$ and $y = u_y\pi^b$ into $y^2 = x(x-1)(x-2)$ and solve for a, b.) A monomial $(x-2)^{-r}y^s$ is in $L(4P)$ only if $2r - s \leq 4$. To avoid having a pole at infinity, we must also have $-2r + 3s \leq 0$. To avoid poles at $(0:0:1)$ and $(1:0:1)$, we take $r \geq 0$ and $s \geq 0$. These conditions give $(r,s) \in \{(0,0),(1,0),(2,1),(2,0),(3,2)\}$, so

$$1, 1/(x-2), y/(x-2)^2, 1/(x-2)^2, y^2/(x-2)^3 \in L(4P).$$

In fact, the functions $\{1, 1/(x-2), y/(x-2)^2, 1/(x-2)^2\}$ form a basis of $L(4P)$.

3.2.2 A basis for the "one-point" spaces $L(mP)$

The ideas in the above examples indicate a method to compute $L(mP)$, for $m \in \mathbb{Z}$ and a point P in a plane curve X. These lead to the following result, for "one-point" Riemann-Roch spaces [4], $L(mP)$. We may, after a change of coordinates, assume P is the "point at infinity" on X.

Lemma 18 *Let X be a plane curve defined by $y^2 = g(x)$, where g is a polynomial of degree d, with d odd. Let $P_0 \in X$ denote the point "at infinity" on X. Assume X is smooth except possibly at P_0. For each $m > d$, the $L(mP_0)$ has a basis consisting entirely of monomials in x and y.*

proof: Note that the genus of X is $g = (d-1)/2$. As in Example 16, we see that on the curve X, x has a pole of order 2 at infinity and y has a pole of order d at infinity. Remark 3 (see also (1) above) gives us $x^{-a}y^{-b} \in L(mP_0)$, provided $2a + db \leq m$, $0 \leq a$, $0 \leq b$. Since d is odd, the only integers not of the form $2a + db$ are those odd integers less than d. Thus there are $m + 1 - (d-1)/2 = m - g + 1$ such integers. The corresponding monomials all have distinct order, hence must be linearly independent. Since m is large, the Riemann-Roch theorem implies that they form all the basis vectors of $L(mP_0)$. $\Box$

Proposition 19 *Let X be a plane curve defined by $y^2 = g(x)$, where g is a polynomial of degree d, with d odd. Suppose $G \subset \mathrm{Aut}(X)$ is a finite subgroup and that the point "at infinity" $P_\infty \in X$ on X is fixed by G. For each $m > d$, the action of G on $L(mP_\infty)$ may be represented by an upper-triangular matrix, with respect to a suitable basis.*

[4] Such spaces are frequently used in applications to the construction of Goppa codes, so this result may be of special interest.

proof: The group G acts on each space in the series

$$\langle 1\rangle = L(P_\infty) \subset L(2P_\infty))\rangle = \langle 1, x\rangle \subset ... \subset L(mP_\infty) \subset ... \,.$$

In particular, G acts on the space $\langle x\rangle \cong L(2P_\infty)/L(P_\infty)$ (the quotient representation). If σ denotes this representation then $\sigma(g)(x) = \chi_\sigma(g)x$, for some character χ_σ of G. This is the action of G on $\langle x\rangle$.

Next, we want to determine the action of G on $\langle y\rangle$. Let $k > 1$ be the smallest integer for which a term of the form y occurs in $L(kP_\infty)$. The group G must act on $\langle y\rangle \cong L(kP_\infty)/L((k-1)P_\infty)$. If τ denotes this representation then $\tau(g)(y) = \chi_\tau(g)y$, for some character χ_τ of G. Thus, G acts on $\langle x^i y^j\rangle$ by $\sigma(g) = \sigma^i\tau^j$. Since $L(mP_\infty)$ has a basis consisting of monomials in x, y, the proof is complete. □

3.3 The general case

The following is our most general result.

Theorem 20 *Let X be a smooth projective curve defined over a field F. Suppose $G \subset \mathrm{Aut}(X)$ is a finite subgroup, and that the divisor $D \neq 0$ on X is stable by G. Let d_0 denotes the size of a smallest orbit of G acting on X. Each irreducible composition factor of the representation of G on $L(D)$ has dimension $\leq d_0$.*

Remark 4 *1. This is best possible in the sense that irreducible subspaces of dimension d_0 can occur, by Theorem 6.*

2. If F has characteristic 0 then every finite dimensional representation of a finite group is semi-simple (Prop 9, ch 6, [Se1]). If F has characteristic p and p does not divide $|G|$ then every finite dimensional representation of G is semi-simple (Maschke's Theorem, Thrm 3.14, [CR], or [Se1], §15.7).

proof: Let $D_0 \neq 0$ be a effective G-invariant divisor of minimal degree d_0. Let $d = [\deg(D)/d_0]$ denote the integer part. The group G acts on each space in the series

$$\{0\} = L(-(d+1)D_0 + D) \subset L(-dD_0 + D) \subset L(-(d-1)D_0 + D) \subset \\ ... \subset L(-(d-m)D_0 + D) \subset ... \subset L(D)\ .$$

In particular, G acts on the successive quotient spaces

$$L(-(d-m-1)D_0 + D)/L(-(d-m)D_0 + D), \quad 0 \leq m \leq d-1,$$

by the quotient representation. These are all of dimension at most d_0 (Prop. 3, ch 8, [F]).

□

Corollary 21 *Suppose that G is a non-abelian group acting on a smooth projective curve X defined over an algebraically closed field F and assume $\pi : X \to X/G$ is unramified* [5]*. Let d_0 be as in the above theorem and let d_G denote the largest degree of all irreducible (F-modular) representations of G. Then*

$$d_0 \geq d_G.$$

proof: Construct an effective divisor D of X fixed by G. By multiplying by a positive integer, we may assume that the degree of D is greater than twice the genus of Y. In this case, it is known (see §3 of Nakajima [N] or §4.7 of Borne [Bo3]) that $L(D)$ is a free $F[G]$-module. In other words, $L(D) \cong F[G]^\ell$, for some $\ell > 0$. Therefore the set of irreducible subrepresentations of $L(D)$ are the same as the set of irreducible representations of G. The result now follows from our theorem.

Here's a second proof, by B. Koeck (private communication, included by permission): If the action is free (which is the same as unramified) then, by definition, d_0 equals the order of G. Hence $d_0 \geq d_G$, since every irreducible representation is a direct summand of the regular representation by classcial representation theory.

□

Example 22 *Let X be a smooth projective curve defined over a field F. Suppose*

- *$G \subset \mathrm{Aut}(X)$ is a finite subgroup,*
- *$X(F)^G \neq \emptyset$,*
- *either $\mathrm{char}(F) = 0$ or $p = \mathrm{char}(F)$ does not divide $|G|$, and*
- *the divisor D on X is stable by G.*

Then the natural representation of G on $L(D)$ decomposes as a direct sum of one-dimensional subrepresentations.

[5] One may also assume G acts freely on X.

Indeed, if $X(F)^G \neq \emptyset$ and the cover $\pi : X \to X/G$ is tamely ramified then G must be cyclic (see Serre [Se2] Corollary 1, ch IV, §2 or Fait 4.4 in Borne [Bo1]), so it's irreducible representations are all 1-dimensional. The fact that $L(D)$ decomposes as a direct sum of one-dimensional subrepresentations also follows from the above theorem and Maschke's theorem.

Example 23 *Let $k = \mathbb{C}$, let $X = X(p)$ be he modular curve of Example 14, where $p \geq 7$ is a prime, and let $G = PSL(2, \mathbb{F}_p)$. The representations of this simple group are described, for example, in Fulton and Harris [FH]* [6]*. In this case, we have, in the notation of the above corollary, $d_G = p + 1$.*

Example 24 *Let X_0 be a smooth projective curve over an algebraically closed field F. Let $K_0 = F(X_0)$ be the function field of X_0. Consider a Galois extension K/K_0 with Galois group $G = Gal(K/K_0)$. Let X be a smooth projective curve such that $K = F(X)$, so $G \subset Aut_F(X)$. Let G_P denote the decomposition group of P in G.*

We claim that there is a Kummer extension X/X_0 of degree ℓ (ℓ a prime distinct from $char(F)$) and a point P of X for which $G_P = G$. This follows from Proposition III.7.3 and Theorem III.8.2 in Stichtenoth [Sti]. (The idea is that the Galois group G is known explicitly, it is a cyclic group of order ℓ, and the order of G_P is known precisely for such "Kummer covers".)

The above corollary in this example says that the all the irreducible subrepresentations representations of G on $L(mP)$ are 1-dimensional.

Example 25 *Let $\mathbb{F}$ be a separable algebraic closure of $\mathbb{F}_3$. Let X denote the Fermat curve over $\mathbb{F}$ whose projective model is given by $x^4 + y^4 + z^4 = 0$. The point $P = (1 : 1 : 1) \in X(\mathbb{F})$ is fixed by the action of S_3.*

Based on the Brauer character table of S_3 over $\mathbb{F}_3$ (available in GAP [GAP]), the group G has no 2-dimensional irreducible (modular) representations.

Definition 26 *Let ρ denote the representation of G on $L(D)$ as in the above theorem. Let χ_1, ..., χ_ℓ denote the distinct characters (of the irreducible subrepresentations) which occur in the decomposition of ρ. We call these the* **characters of** *D.*

[6] Actually those of $SL(2, \mathbb{F}_p)$ are described in [FH], but it is easy to determine the representations of $PSL(2, \mathbb{F}_p)$ from those of $SL(2, \mathbb{F}_p)$.

For more on the relationship between the characters of D, the geometry of X, and the divisor D itself, see [MP] for the case $D = K$ and $F = \mathbb{C}$ and Theorem 4.5 in Köch [K] in general. For the case where χ_i is one-dimensional, see also §2 of Kani [Ka].

It would be interesting to know more precise information than that given in Corollary 21.

Question: Are there general conditions for which $d_0 = d_G$ holds?

Question: Is there an analog of Corollary 21 for tamely ramified $\pi : X \to X/G$?

4 Applications

In this section we discuss a possible application to coding theory.

Throughout this section, we assume X, G, and D are as in Theorem 20. Assume F is finite.

Let $E = P_1 + ... + P_n \in Div(X)$ be stabilized by G, where $P_i \in X$. Assume $\mathrm{supp}(D) \cap \mathrm{supp}(E) = \emptyset$. Let $C = C(D, E)$ denote the Goppa code

$$C = \{(f(P_1), ..., f(P_n)) \mid f \in L(D)\}.$$

The group G acts on C by $g \in G$ sending $c = (f(P_1), ..., f(P_n)) \in C$ to $c' = (f(g^{-1}(P_1)), ..., f(g^{-1}(P_n)))$. This induces a homomorphism of G into $\mathrm{Aut}(C)$, denoted $\phi : G \to \mathrm{Aut}(C)$ (Prop. VII.3.3, [Sti], and §10.3, page 251, of [St])[7].

To investigate the kernel of this map ϕ, we introduce the following notion. Let $H \in Div(X)$ be any divisor. We say that the space $L(H)$ **separates points** if for all points $P, Q \in X$, $f(P) = f(Q)$ (for all $f \in L(H)$) implies $P = Q$ (see [H], chapter II, §7, for more details on this concept). If $L(D)$ separates points then

$$\mathrm{Ker}(\phi) = \{g \in G \mid g(P_i) = P_i,\ 1 \leq i \leq n\}.$$

For example, if X is a plane curve and if the field generated by $L(D)$ contains the coordinate functions x, y then $L(D)$ separates points. It is known (proof of Prop. VII3.3, [Sti]) that if $n > 2g+2$ then $\{g \in G \mid g(P_i) = P_i,\ 1 \leq i \leq n\}$

[7] Both of these references make the mistake of defining ϕ by $\phi(g)(c) = (f(g(P_1)), ..., f(g(P_n)))$. However, this is not a homomorphism.

is trivial. Therefore, if $n > 2g + 2$ and $L(D)$ separates points then ϕ is injective.

Suppose G permutes the $\{P_i\}$. Then $\phi(g)$ may be represented by a permutation matrix acting on the F-vector space C. Let ρ be as in §1 and assume F contains all the N^{th} roots of unity, where $N = |G|$. For f in a suitable basis of $L(D)$, $\rho(g)f = \chi(g)f$, for some character $\chi : G \to F^\times$. Then $\phi(g)(c) = (\rho(g)f(P_1), ..., \rho(g)f(P_n)) = \chi(g)(f(P_1), ..., f(P_n))$. We have two expressions for the image of c:

$$\phi(g)(c) = (f(g^{-1}(P_1)), ..., f(g^{-1}(P_n))) = \chi(g)c,$$

where f is in a suitable basis of $L(D)$.

This extra symmetry of the code may be useful in practice. For example, it can be used to more efficiently store codewords in memory on a computer.

Example 27 *Let $G = S_3$ act on the genus 3 Fermat quartic X whose projective model is $x^4 + y^4 + z^4 = 0$ over $\mathbb{F}_9 = \mathbb{F}_3(i)$, where i is a root of the irreducible polynomial $x^2 + 1 \in \mathbb{F}_3[x]$. One can check that there are exactly 6 distinct points in the G-orbit of $[-1 : i : 1] \in X(\mathbb{F}_9)$. Let*

$$G \cdot [-1 : i : 1] = \{Q_1, ..., Q_6\},$$
$$E = Q_1 + ... + Q_6 \in Div(X), \quad D = 6 \cdot [1 : 1 : 1] \in Div(X).$$

Then $L(D)$ is 4-dimensional, by the Riemann-Roch theorem. Note that no Q_i belongs to the support of D, so we may construct the Goppa code

$$C = \{(f(Q_1), ..., f(Q_6)) \mid f \in L(D)\},$$

a generator matrix being given by the 4×6 matrix $M = (f_i(Q_j))_{1 \le i \le 4, 1 \le j \le 6}$, where $f_1, ..., f_4$ are a basis of $L(D)$. According to MAGMA [MAGMA], $dim_{\mathbb{F}_9}(C) = 3$ and the minimum distance of C is 4. (According to [Br], this is best possible.) The action of an element in the group G on C permutes the Q_i, hence may be realized by permuting the coordinates of each codeword in C in the obvious way. (In other words, the action of G on C is isomorphic to the regular representation of S_3 on itself.) Using the group action, storing all $|C| = 9^3 = 729$ elements may be reduced to storing only the representatives of each orbit C/S_3.

If instead of taking for the divisor E the sum of all the points in the orbit of $[-1 : i : 1]$, we take

$$E = \sum_{P \neq [1:1:1], P \in X(\mathbb{F}_9)} P,$$

so E is of degree $|X(\mathbb{F}_9)| - 1 = 27$, then the general theory (in §3.2.3 of [TV]. for example) gives that the associated Goppa code C has length 27*,* $dim_{\mathbb{F}_9}(C) = 4$ *and the minimum distance of C is* 21*. (According to [Br], this is best known.)*

Acknowledgements: We thank Keith Pardue, Caroline Melles, Niels Borne, and Niranjan Ramachandran for useful comments. We thank Nick Sheppard-Barron for the reference to [MP]. Finally, we especially thank Bernhard Köck for many detailed comments improving the content of the paper and for the references [Ka], [K].

References

[Bo1] N. Borne, “Une formule de Riemann-Roch equivariante pour des courbes,” preprint 1999

[Bo2] —–, “Structure de groupe de Grothendieck équivariant d'une courbe et modules galoisiens,” preprint

[Bo3] —–,“Modules galoisiens sur les courbes: une introduciton,” Sém. et Congrès, SMF $\underline{5}$(2001)147-159.

[B] T. Breuer, **Characters and automorphism groups of Riemann surfaces**, London Math. Soc. Lecture Notes, 1999.

[Br] W. Brouwer's tables on Bounds on the minimum distance of linear codes, `http://www.win.tue.nl/~aeb/voorlincod.html`
See also W. Brouwer's (less up-to-date) article in **Handbook of coding theory**, (ed. Pless et al), North-Holland, Elsevier, (1998).

[CR] C. Curtis, I. Reiner, **Methods of representation theory, I**, Wiley-Interscience, 1981.

[F] W. Fulton, **Algebraic curves**, Benjamin, 1969.

[FH] —— and J. Harris, **Representation theory: a first course**, Springer-Verlag, 1991.

[GAP] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.3*; 2002,
(`http://www.gap-system.org`).

[G] V. D. Goppa, **Geometry and codes**, Kluwer, 1988.

[H] R. Hartshorne, **Algebraic geometry**, Springer-Verlag, 1977.

[Ka] E. Kani, "The Galois-module structure of the space of holomorphic differential forms on a curve," J. reine angew. Math $\underline{367}$(1986)187-206.

[K] B. Köck, "Galois structure of Zariski cohomology for weakly ramified covers of curves," math.AG/0207124, available at `http://front.math.ucdavis.edu/`

[Le] J. Lewittes, "Automorphisms of compact Riemann surfaces," Amer. J. Math. $\underline{35}$(1963)734-752.

[L] D. Lorenzini, **An invitation to arithmetic geometry**, Grad. Studies in Math, AMS, 1996.

[MAGMA] W. Bosma, J. Cannon, C. Playoust, "The MAGMA algebra system, I: The user language," J. Symb. Comp., $\underline{24}$(1997)235-265. (`http://www.maths.usyd.edu.au:8000/u/magma/`).

[MP] I. Morrison and H. Pinkham, "Galois Weierstass points and Hurwitz characters," Annals of Math., $\underline{124}$(1986)591-625.

[N] S. Nakajima, "Galois module structure of cohomology groups of an algebraic variety," Inv. Math. $\underline{75}$(1984)1-8

[Se1] J.-P. Serre, **Linear representations of finite groups**, Springer-Verlag, 1977.

[Se2] ——, **Local fields**, Springer-Verlag, 1977.

[SKKT] K. Smith, L. Kahanpää, P. Kekäläinen, W. Traves, **An invitation to algebraic geometry**, Springer-Verlag, 2000.

[St] S. Stepanov, **Codes on algebraic curves**, Kluwer, NY, 1999.

[Sti] H. Stichtenoth, **Algebraic function fields and codes**, Springer-Verlag, 1993.

[TV] M. Tsfasman, S. Vladut, **Algebraic-geometric codes**, North-Holland, 1998.

[W] A. Weil, **Basic number theory**, Springer-Verlag, 1975.